An Image Forensic Technique for Detection of Copy-Move Forgery in Digital Image

Ashwini Malviya(✉) and Siddharth Ladhake

Sipna College of Engineering and Technology, Amravati, India
ash.malviya@gmail.com, sladhake@yahoo.co.in

Abstract. Image morphing is a common practice nowadays. To validate a digital image is considered as a perplexing task in the field of image forensic. With numerous kind of tampering been carried out on a digital image, the paper focuses on a detection of common forgery referred to as copy-move forgery or cloning, which is nearly untraceable. The paper contemplates on the color content of the forged image and employs three different methods of feature extraction to aid the detection of forgery. The experimental results show that the feature extraction methods employed detects the forged region accurately and are also effective to rotation and scaling. A performance analysis in detection of forgery for the three methods in terms precision and recall is also presented in the paper, along with a comparison with other state-of-the-art detection methods.

Keywords: Forgery detection · Digital Forensics · copy-move forgery detection

1 Introduction

In the arena of image forensic, the confirmation of a digital image has been a thought-provoking assignment. With thriving technology, the usage of refined cameras and photo editing software has risen. A smart phone itself has different user-friendly options to alter a picture captured, as desired. It becomes tedious to identify an altered image from the real image as it has become very easy to tamper an image. Scrutiny of all kind of evidence is an inevitable part of Forensic science. The legal system banks on the forensic examination.

A digital image can be forged, by adding, deleting or changing an object in the image, or it can be spliced with other image. The forgery taken into consideration here is the copy-move forgery also referred as cloning. In this kind of tampering, any undesired content of the image can be hidden by pasting a portion copied from the same image on the object. The image contents also can be enriched by cloning.

Though this cloning is not traceable by a common viewer, it creates glitches in the statistics of the pixels of the image. In forensic pertaining to digital image, the pixel plays a crucial role. The changes occurring in these pixel values on tampering can aid the detection of the forgery. The digital forensics investigation is carried out by active and passive approaches. Unlike the active detection approach, the paper presents a passive approach for detection of forgery which works in absence of watermark. The approach explores the HSV histogram, color moment and auto color Correlogram for

P. Mueller et al. (Eds.): SSCC 2016, CCIS 625, pp. 328–335, 2016.
DOI: 10.1007/978-981-10-2738-3_28

feature extraction. These extraction methods are extensively employed in image retrieval systems. In the rest of the paper we discuss the different state-of-the-art techniques for copy-move tampering detection, followed by the proposed approach and the experimental results followed by conclusion.

2 Related Work

Extensive research is been carried out in past few years for copy-move forgery detection. In this segment we probe into different techniques used for the forgery detection. The traditional methodology for the detection scheme starts with usually dividing the image into overlapping blocks, with specific block size. The block based methods implemented by [2, 3] uses DCT coefficient and PCA for extracting features from each block respectively. Further the matrix formed is lexicographically sorted for identifying the duplicated region.

A robust detection technique proposed by W. Luo et al. [4], derived the block characteristics of each block and compared it with other blocks to get the match. These methods were computationally less complex but failed in detection at event of variation arising due to noise and compression. A Keypoint based method [6, 10] uses Scale Invariant Feature Transform algorithm for detection of copy-move forgery.

DWT and SVD based detection technique proposed by G. Li et al. [5], gives a reduced dimension representation. The sorting is simpler and the technique is robust to retouching and compression. N. Myna et al. [7] also presented reduced dimension representation by determining the wavelet transform of the image. The detection of forgery is based on extracting log polar coordinates and phase correlation.

Extraction of features by calculating the Fourier-Mellin Transform of the blocks of the image was proposed by Bayram et al. [9]. The attributes of Fourier Mellin transforms were analyzed in this method, also counting bloom filter was preferred over lexicographically sorting.

Jing-Ming Guo et al. [12] proposed an efficient detection technique using improved daisy descriptor. The method also incorporates adaptive non-maximal suppression for matching of keypoints. This descriptor used is rotation invariant and therefore can detect duplicated region which have been subjected to any kind of transformation. Leida Li et al. [13] used Polar Harmonic transform of circular block for feature extraction. The match was detected on post processing the image.

A detection scheme which involved feature extraction of blocks by histogram of Gabor magnitude was proposed by Chen-Ming Hsu et al. [14]. Like [13] the match was detected on applying post processing operations. Recently Cheng-Shian Lin et al. [15] reduced the computational time by 10% by introducing the cluster expanding block algorithm for detection of duplicated region. In a recent prior work [16] analyzed the color contents of the image for feature extraction which efficiently reduces the complexity.

3 Proposed Scheme

The proposed scheme as illustrated in Fig. 1, first preprocesses the input image, followed by dividing the image into blocks. Often to make the tampering imperceptible the copied region is rotated or flipped or subjected to some other transformation before pasting, therefore we subject each block to transformations. Further the features are extracted from each block. The extracted features form an array, features of each block is matched with every other block to identify the cloning. The match detection is done by using suitable similarity measure.

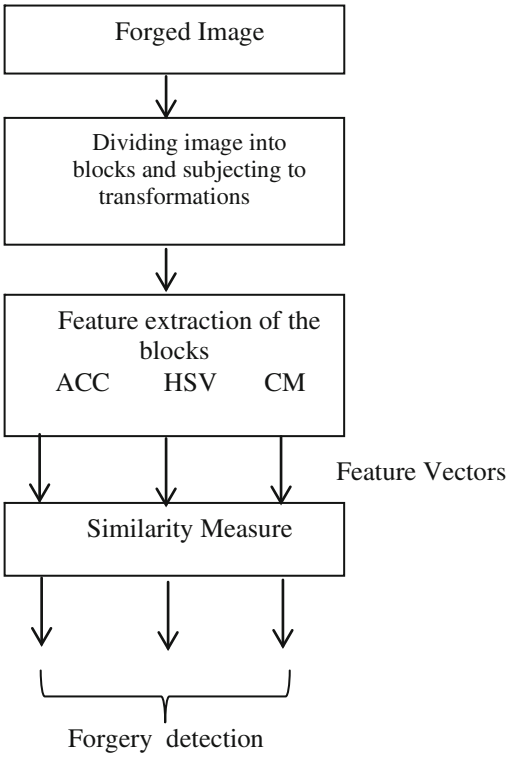

Fig. 1. Functional Flow diagram for proposed scheme

Preprocessing the image involves filtering the noise from the image and dividing the image into blocks. Dividing the image into blocks has been traditional in cloning detection methods. We divide the image of size m x n, into overlapping blocks of size m/4 x n/4. Each block is subjected to 8 transformations, mainly rotation, flipping and transpose. Features are extracted from each block. Features are extracted by computing the HSV histogram, color moments and auto color Correlogram of each block.

HSV Histogram. As we focus on the pixel for forgery detection, the HSV color space can be well analyzed for varying values of the Hue, Saturation and Intensity of pixel.

The image is first split into H, S, and V plane and then each plane is quantized, specifying the number of quantization levels. A final histogram is created and then normalized.

Color Moments. Color feature vectors are derived from the RGB model, the scheme takes into account two color moments. The first color moment namely mean and the second moment namely standard deviation are computed for each channel. The mean and the standard deviation are defined as follows:

$$\mu = \frac{1}{M}\sum_{i=1}^{M} f_i \;\; \sigma = \sqrt{\frac{1}{M}\sum_{i=1}^{M}\left(f_i - \mu\right)^2} \tag{1}$$

AutoColorCorrelogram (ACC). The AutoColorCorrelogram was introduced by [8] for spatial color indexing. It computes the mean color by taking in consideration all the pixels of a particular color, say C_j at a distance k from all pixels of another color, say C_i. It can be defined as follows:

$$ACC(i,j,k) = Avg\gamma^{(k)}_{C_i VC_j}(I) = \left\{ Avg\gamma^{(k)}_{C_i C_{jr}}(I), Avg\gamma^{(k)}_{C_i C_{jg}}(I), Avg\gamma^{(k)}_{C_i C_{jb}}(I) \middle| C_i \neq C_j \right\} \tag{2}$$

Where the mean colors are formulated as follows:

$$Avg\gamma^{(k)}_{C_i C_{jx}}(I) = \left. \frac{\prod^{(k)}_{C_i C_{jx}}(I)}{\prod^{(k)}_{C_i C_{jx}}(I)} \right| x = r, g, b \tag{3}$$

The image here is quantized into m colors. VC_j implies, RGB value of color m.

Forgery Detection. Manhattan distance or commonly referred as L1 norm is used as a similarity measure for comparing the features of each block with every other block. The features of each block are arranged in a row of a matrix. The L1 measure requires less computational time as compared to Euclidean distance. Its simplicity and robustness makes it more appropriate for match detection. If $a=(x_1,x_2,..x_n)$ and $b=(y_1,y_2,\ldots y_n)$ the Manhattan distance is obtained by,

$$MH(a,b) = \sum \left|x_i - y_i\right| \quad = \quad \text{for i } = 1, 2 \ldots, \text{ n.} \tag{4}$$

The distance is calculated by taking sum of absolute difference between the considered block feature vectors and all other blocks feature vectors. Then the resultant matrix is sorted to find the least difference row.

4 Visual Results

The detection scheme developed is tested on few images which are created individually and on image database CoMoFoD which is made available online by [17]. The database comprises of set images of small and large categories, where the images are subjected

to various alterations viz. rotation, scaling, distortion, translation and combination of the same. We have considered the image set which is small image category (512×512). Figure 2 consist of three images, wherein the first image is the original image, the second image is forged image, and wherein a portion of image is copied and rotated earlier to pasting in the same image, and a duplicated region is identified by using ACC for feature extraction in the next image. The images in Figs. 3, 4 and 5 are from the CoMoFoD database.

Fig. 2. Original image, forged image and forgery detected using ACC. The forged region has undergone rotation prior to pasting.

Fig. 3. Original image, forged image (cloned region scaled) and forgery detected using ACC.

Fig. 4. Original image, forged image (plain copy move) and forgery detected using Color moments

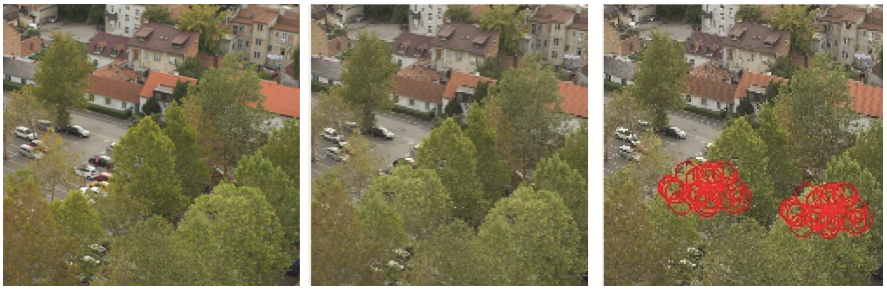

Fig. 5. Original image, forged image and forgery detected by extracting HSV Histogram of each block.

Figure 3 depicts a forgery detection using ACC where the forged part is scaled before pasting.

Figure 4 depicts detection of copy-move forgery using color moments of the blocks for feature extraction.

The forgery is detected for the image in Fig. 5 using HSV Histogram, combinational transformations is used to tamper the image.

5 Metric and Statistical experimental Results

The performance analysis is carried out at image level. The performance assessment is based on the false and true outputs. The precision P and recall R is computed as follows:

$$P = \frac{T_p}{T_p + F_p} \quad R = \frac{T_p}{T_p + F_n} \quad F_1 = \frac{2PR}{P + R} \tag{5}$$

T_p represents the number of forged images detected correctly; F_p represents the number of images incorrectly detected as forged and F_n indicates the falsely missed tampered images. The combinational measure of precision and recall is given by F_1. Table 1 gives the performance analysis of about 200 images from the CoMoFoD database, which consists of 100 forged and 100 original images. The performance analysis in terms of precision for three different methods employed is shown in figure 6.

Table 1. Cloning detection results at image level.

Methods	Tp	Fp	Fn	P (%)	R (%)	F_1
ACC	94	6	6	0.940	0.940	0.940
Color Moments	94	8	6	0.922	0.940	0.931
HSV	92	11	8	0.893	0.920	0.906

AutoColorCorrelogram shows effective detection with precision of 94% when the proposed scheme is tested on images from the database. Also a comparison with state-of-the art methods employed [11] for copy-move forgery detection is presented in graphical form in figure 7.

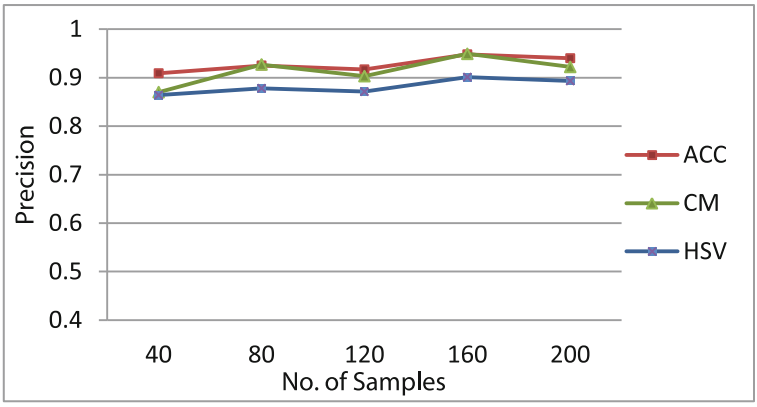

Fig. 6. Comparative analysis based on F1 score.

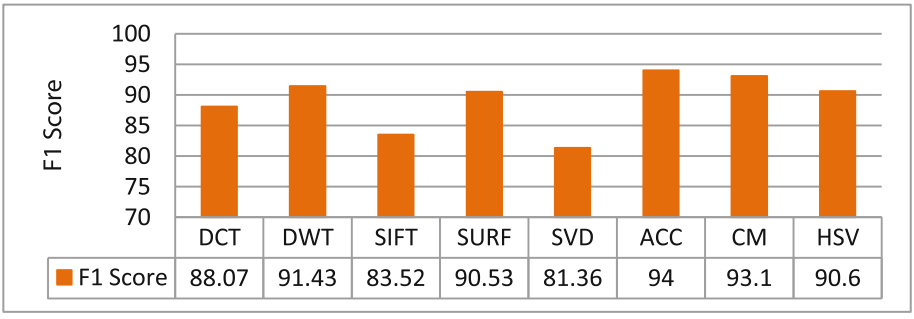

Fig. 7. Comparative analysis based on F1 score.

6 Conclusion

In proposed scheme, an efficient copy move tampering detection technique is developed. The feature extraction methods implemented in the scheme have been employed widely for content based image retrieval earlier. The proposed scheme presents three different detection techniques for copy move forgery detection, which is less complex and provides robustness to transformation and noise. AutoColorCorrelogram shows effective detection with highest precision when the proposed system is confirmed on images from the database. The detection method is also effective in detection of forgery on event of scaling and multiple cloning in the same image.

References

1. Farid, H.: A Survey of Image Forgery Detection. Signal Process. Mag. **26**(2), 16–25 (2009)
2. Fridrich, J., Soukal, D., Lukáš, J.: Detection of copy-move forgery in digital images. In: Proceedings of Digital Forensic Research Workshop, August 2003
3. Popescu, A., Farid, H.: Exposing digital forgeries by detecting duplicated image regions. Department of Computer Science, Dartmouth College, Technical report TR2004-515 (2004). www.cs.dartmouth.edu/farid/publications/tr04.html
4. Luo, W., Huang, J., Qiu, G.: Robust detection of region-duplication forgery in digital images. Int. Conf. Pattern Recogn. **4**, 746–749 (2006)
5. Li, G., Wu, Q., Tu, D., Sun, S.: A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In: IEEE International Conference on Multimedia and Expo, pp. 1750–1753, July 2007
6. Huang, H., Guo, W., Zhang, Y: Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm. In: Pacific-Asia Workshop on Computational Intelligence and Industrial Application, vol. 2, pp. 272–276, December 2008
7. Myna, A.N., Venkateshmurthy, M.G., Patil, C.G.: Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In: IEEE International Conference on Computational Intelligence and Multimedia Applications, pp. 371–377, December 2007
8. Tungkasthan, A., Intarasema, S., Premchaiswadi, W.: Spatial color indexing using ACC algorithm. In: Seventh International Conference on ICT and Knowledge Engineering, pp. 113–117 (2009)
9. Bayram, S., Sencar, H., Memon, N.: An efficient and robust method for detecting copy-move forgery. In: IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 1053–1056, April 2009
10. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G.: A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011)
11. Christlein, V., Riess, C., Jordan, J., Riess, C.: Angelopoulou, E: An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf. Forensics Secur. **7**(6), 1841–1854 (2012)
12. Guo, J.M., Liu, Y.-F., Wu, Z.-J.: Duplication forgery detection using improved DAISY descriptor. Expert Syst. Appl. **40**, 707–714 (2013). Elsevier International Journal
13. Li, L., Zhu, S., Xiaoyue, H.W.: Detecting copy-move forgery under affine transforms for image forensics. Comput. Electr. Eng. **40**(6), 1951–1962 (2014). Elsevier Ltd.
14. Hsu, C.-M., Lee, J.-C., Chen, W-K.: An efficient detection algorithm for copy-move forgery. In: 10th Asia Joint Conference on Information Security, pp 33-36, May 2015
15. Lin, C.-S., Chen, C.-C., Chang, Y.-C.: An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection. In: International Conference on Intelligent Networking and Collaborative Systems (INCOS), pp. 228–231, September 2015
16. Malviya, A.V., Ladhake, S.A.: Pixel based image forensic technique for copy-move forgery detection using auto color correlogram. Procedia Computer Science **79**(2016), 383–390 (2016). In: 7th International Conference on Communication, Computing and Virtualization 2016. Elsevier Ltd.
17. Tralic, D., Zupancic, I., Grgic, S., Grgic, M.: CoMoFoD - new database for copy-move forgery detection. In: Proceedings of 55th International Symposium, ELMAR-2013, pp. 49–54, September 2013